ABSTRACT

The present invention provides a method and apparatus for detecting and preventing a plurality of denial of service (DOS) and distributed denial of service (DDOS) attacks. The apparatus includes classifiers for parsing packets; meters storing statistics for the classified packets and detecting flood thresholds; an Ager for maintaining timeouts; a decision multiplexer for multiplexing inputs from various meters and determines whether to allow or deny the packet; and a threshold estimation means for estimating thresholds based on past data from meters, baselines, trends and seasonality. The apparatus includes a PCI interface through which a host can interact, learn continuously and set thresholds in a continuous and adaptive manner so as to prevent rate based DOS and DDOS attacks. The apparatus includes a mechanism to track culprit sources at layer 2 and layer 3 through a multiplicative increment method.